

Talking to children about data and privacy online: Research methodology



Please cite as: Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) *Talking to children about data and privacy online: research methodology*. London: London School of Economics and Political Science.

The project

With growing concerns over children's online privacy and the commercial uses of their data, it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy.

This project seeks to address questions and evidence gaps concerning children's conception of privacy online, their capacity to consent, their functional skills (e.g., in understanding terms and conditions or managing privacy settings online), and their deeper critical understanding of the online environment, including both its interpersonal and, especially, its commercial dimensions (including its business models, uses of data and algorithms, forms of redress, commercial interests, systems of trust and governance).

The project takes a child-centred approach, arguing that only in this way can researchers provide the needed integration of children's understandings, online affordances, resulting experiences and wellbeing outcomes. Methodologically, the project prioritises children's voices and experiences within the framework of evidence-based policy development by:

- conducting focus group research with children of secondary school age, their parents, and educators, from selected schools around the UK;
- creating an online toolkit to support and promote children's digital privacy skills and awareness;
- organising child juries for evaluating resources to be included in the toolkit and reviewing recommendations for privacy and data-relevant policy and practice.

Contents

| | |
|--|----|
| Part I: Developing the methodology | 3 |
| Conceptual framework | 3 |
| Piloting and adaptation..... | 5 |
| Workshop activities | 6 |
| Child juries | 10 |
| Part II: The research process..... | 12 |
| Ethics approval..... | 12 |
| Recruitment | 12 |
| Data collection | 13 |
| Participants | 14 |
| Data analysis | 15 |
| Coding framework | 15 |
| Appendix | 17 |
| References | 23 |

Part I: Developing the methodology

The methodology was developed based on three elements: a theoretically driven conceptual framework, reviewing the existing research with children, and consulting other research experts on what works well when discussing online privacy with children. The tools were then piloted in two schools and adapted to address the challenges we met.

An initial scoping of the literature during the research proposal stage enabled us to sketch the research approach, design and methods, which were later elaborated on and developed further.

Focus group methodology was proposed because it allows children's voices and experiences to be expressed in a way that is meaningful to them, and permits children to act as agents in shaping their digital rights, civic participation and need for support (Greene and Hogan, 2005; Kleine et al., 2016). The aim was to use real-life scenarios and exemplar digital experiences to facilitate the focus group discussions, and to ensure that children are clearly focused on the opportunities, risks and practical dilemmas posed by the online environment.

Child juries (Coleman et al., 2017; Family, Kids, and Youth, 2017) were proposed to allow children to work creatively and collaboratively with the research findings, enabling them to identify possible solutions to the key online privacy challenges and to select which ideas to be transformed into practical policy and education recommendations. The jury approach aims to allow the bottom-up formulation of public agendas and to open up opportunities for the participation of young people in the debates relevant to them (Coleman et al., 2017). In previous research this method has proved an effective means of child consultation that can inform policy and practice development in a way that is close to children's lives and current concerns.

The first stage of the project involved using systematic evidence mapping to review the existing knowledge on children's data and privacy online, identify research gaps and outline areas of potential policy and practice development. The process of evidence mapping was helpful in pinpointing the key areas where more research is needed and relevant methodological approaches and tools. We also consulted a number of researchers whose projects seemed particularly relevant in terms of research topic or methodology. This enabled us to design a **conceptual framework** that was used to design focus group schedules and activities.

Conceptual framework

1. Drawing on Nissenbaum's (2004) notion of *privacy as contextual integrity* we understand privacy online as depending on the context (itself interesting in the digital environment, with its many and changing apps and services). This prioritises the judgement (especially, by the data subject) of what it is appropriate to share within particular contexts or relationships – particularly important in digital environments where respect for the child's perspective is easily neglected. Hence, we designed the research tools in a way to capture the context in which children make decisions about their data and privacy online – seeking to understand both what they do and why (for details, see Livingstone et al., 2019).

2. To capture the full complexity of children's privacy and data online, we distinguish among *three types of privacy*:
 - (i) **interpersonal privacy** – how my 'data self' is created,¹ accessed and multiplied via my online social connections;
 - (ii) **institutional privacy** – how public agencies like government, educational and health institutions gather and handle data about me;
 - (iii) **commercial privacy** – how my personal data is harvested and used for business and marketing purposes.

Distinguishing interpersonal, institutional and commercial contexts helps resolve the (somewhat dismissive) privacy paradox – namely, that young people *say* they care about their privacy yet in practice they *share* personal information on public platforms.

The focus group schedules and activities were designed in a way to capture all three areas.

3. To conceptualise what children know and expect in relation to data, we adapted a typology from privacy lawyer Simone van der Hof (2016), distinguishing *three types of children's online data*:
 - (i) **data given** – the data contributed by individuals (about themselves or about others), usually knowingly though not necessarily intentionally, during their participation online;
 - (ii) **data traces** – the data left, mostly unknowingly – by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata;
 - (iii) **inferred data** – the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources.

We were interested in capturing children's practices and competences related to all three types of data, and designed the research tools in a way to elicit them. Thus, the focus group discussions covered the following key areas (see also the Appendix):

- Internet use and privacy awareness (apps, sites and devices used by children; general privacy awareness and practices; decision-making and parental supervision, trust).
- Privacy knowledge (key privacy-related terms and their application).
- Children's data sharing (children's practices and views around sharing data related to web browsing, internet searches, preferences, location, health records, personal and identity information, biometric data, social networks, personal habits, finances, school records and sensitive information). Preferences of who they might share it with (e.g.,

¹ 'Data self' refers to all the information available (offline and online) about an individual.

their online contacts; school, GP, future employer; commercial companies) or decide to keep to themselves and why.

- Children's data profiling (understanding of profiling, reflections, concerns and harm, limitations to profiling).
- Children's privacy strategies and support (practices and experiences of protecting and controlling personal information; learning, support and help-seeking).
- Questions and advice (what other children should know about the internet, suggestions and questions to governments, educators, parents, industry, researchers).

The designing of the research tools involved developing focus group and interview schedules and activities for children, parents and teachers. The project team developed several drafts of the tools that were discussed with experts working on privacy or children's use of digital technologies and improved, based on the feedback. The focus group and interview schedules were then piloted and finalised.

Piloting and adaptation



The research tools were piloted in two average-performing London schools with a mixed pupil population. The schools were contacted via snowballing from personal contacts, and selected based on interest in participation. The piloting enabled us to try out and revise the activities and to test the approximate duration of the focus group, allowing some flexibility by designing additional activities for the cases when we had more contact time with the participants.

The testing of the materials demonstrated some challenges in researching children's privacy online – children found it hard to discuss institutional and commercial privacy, as well as data profiling, as they seemed to have substantial gaps in their understanding of these areas. They also did not see their online activities as data or as sharing personal information online. This made it hard to establish how important privacy was for them and what digital skills they had.

To address this, the team took a step-by-step approach – starting with the unprompted perceptions of privacy and children's practices (e.g., in relation to selecting apps, checking age restrictions, reading terms and conditions, changing privacy settings, getting advice about new apps from others) and a quick test of their familiarity with relevant terminology (e.g., cookies, privacy settings, algorithms, facial recognition). They then moved on to more complex areas, such as types of data they share and with whom, gradually building the

landscape of children's online behaviour and enabling discussion of less thought-of areas such as data harvesting and profiling.

Workshop activities

An activity that worked really well as an introduction was asking children about the apps and websites they use – this quickly produced a comprehensive picture of their recent activities and the platforms they engage with (see Figure 1). The examples of the apps children use then offered an opportunity to ask about their practices in a more contextualised and familiar setting, rather than talking about the internet more generally, which children found harder.

Figure 1: What apps and websites did you use over the past week?



This first activity was then used to talk about children's understanding of privacy, their practices, and to introduce issues such as trust, age-appropriate design, parental mediation and the 'right age' for children's independent use, before moving on to children's familiarity with privacy-related terminology (see Figure 2 below). This enabled the team to allow the children to talk about their experiences on their own terms, and to introduce gradually more complex privacy issues, such as data sharing.

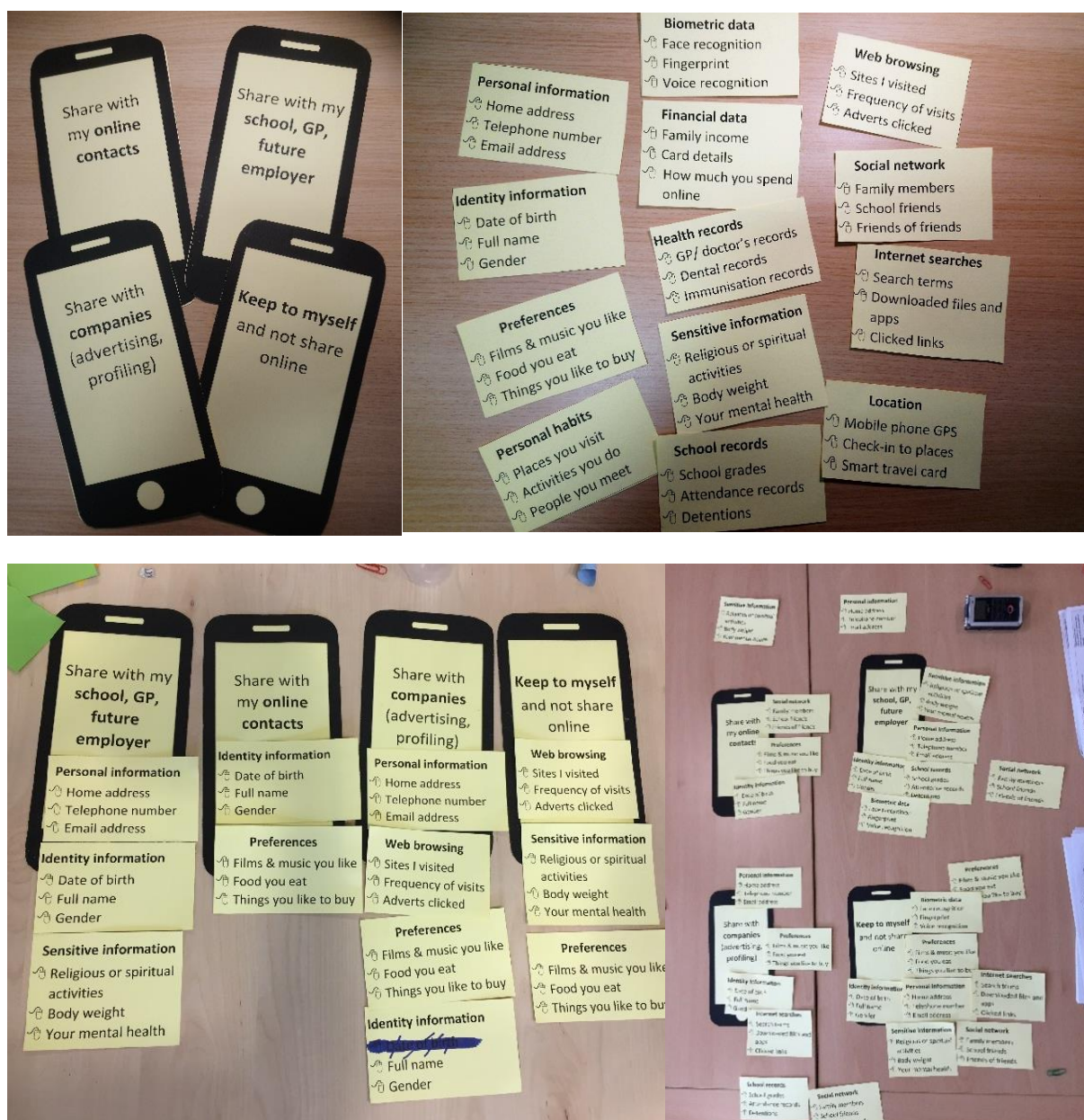
Figure 2: Have you heard this word? Can you tell me what it means? (words introduced one at a time)



Another challenge was to help the children describe what they share online and their understanding of how additional information might be collected in the background by the apps and used to create a digital profile. The initial idea to ask children to brainstorm about all the data they might have shared with prompts from the team was not very effective. The children came up with a limited number of items, such as name and photos, but needed a lot of prompting to think about other data, such as location, preferences or biometric data. Institutional collection of their data, such as by the school or their GP, was rarely considered. We were also interested in a more nuanced understanding of why and how children share the data, and their reflections on the possible implications, but this was hard to elicit.

The team therefore restructured the activities, making them more visual and interactive (see Figure 3). This enabled the children to engage better with the different dimensions of privacy online and to relate their experiences to the issues discussed.

Figure 3: Online data activities



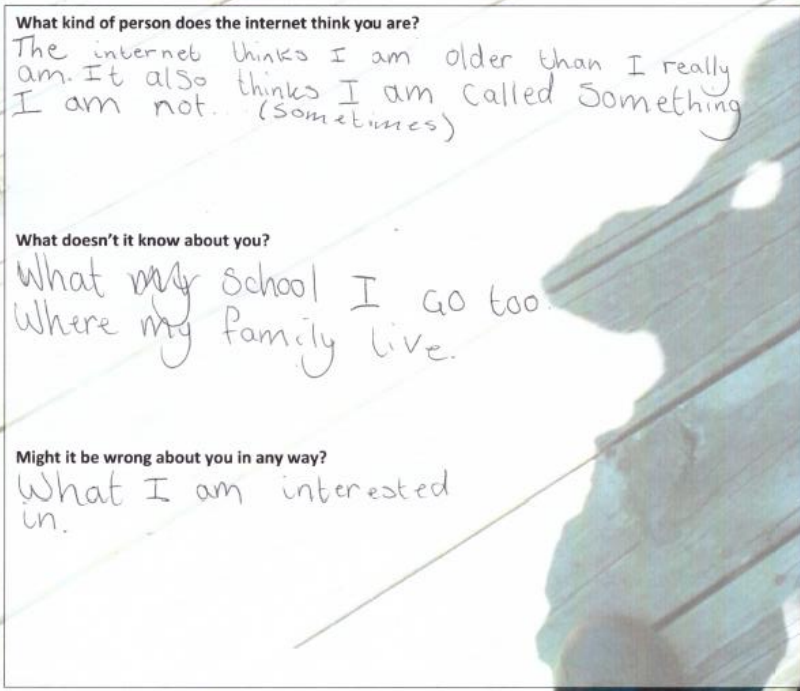
The children were given four sharing options – share with online contacts (interpersonal privacy), share with my school, GP, or future employer (institutional privacy), share with companies (commercial privacy), and keep to myself (desire not to share something). We identified 13 types of data that might be shared digitally (personal information, identity information, preferences, personal habits, biometric data, web browsing, social network data, internet searches, location, financial data, health records, school records or sensitive information).² These were later simplified further to the current nine most relevant groups.

The children were then asked to say whether they share each type of data with anyone, why they might share it and what the implications of this might be. This worked really well as it allowed them to relate the examples to the applications they use and to some practical situations (e.g., sharing information about their address with a delivery app). It also helped the children to think if they are happy to share this data and under what circumstances, or whether they would prefer to keep it to themselves. Interestingly, this exercise demonstrated that children often choose ‘keep to myself’ spontaneously but, as the discussion progressed, they acknowledged that they are sometimes asked for this data and feel obliged to provide it. This enabled consideration of both voluntary and involuntary sharing of data and also the collection of data by apps ‘in the background’.

Having all the data they have shared on the table in front of them was also helpful when next prompting the children to reflect on what the internet knows about them (see Figure 4) and to think about the possible implications of this.

Figure 4: What does the internet know about you?

What does the internet know about you? This is sometimes called your data shadow or data footprint. Write your answers below.



What kind of person does the internet think you are?
 The internet thinks I am older than I really am. It also thinks I am called something I am not. (Sometimes)

What doesn't it know about you?
 What my school I go too.
 Where my family live.

Might it be wrong about you in any way?
 What I am interested in.

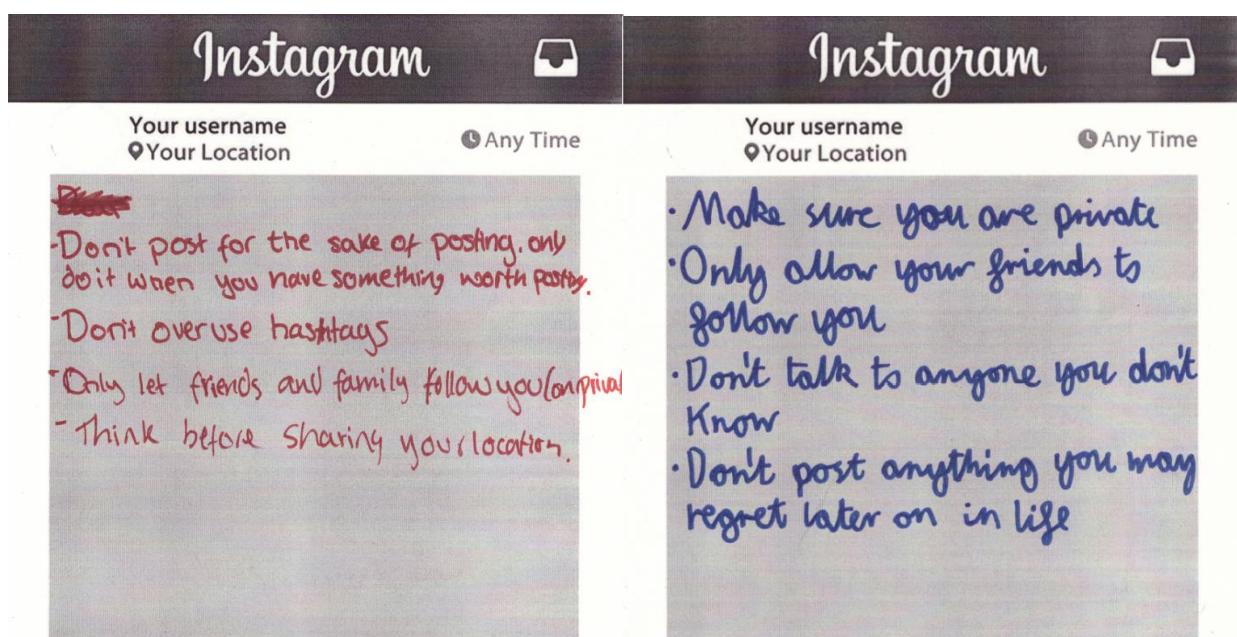
Are you a girl or boy? Girl How old are you? 12

² We adapted the data cards developed by the UnBias project (<https://unbias.wp.horizon.ac.uk/fairness-toolkit/>) after consultation with the team.

Still, thinking about the possible future implications remained a challenge. The discussion often diverted to general internet safety, with the children reciting familiar messages about 'stranger danger' and password sharing, but failing to grapple with how their data might become available online and how it might be used for unintended purposes. Much prompting was used to elicit greater details about this.

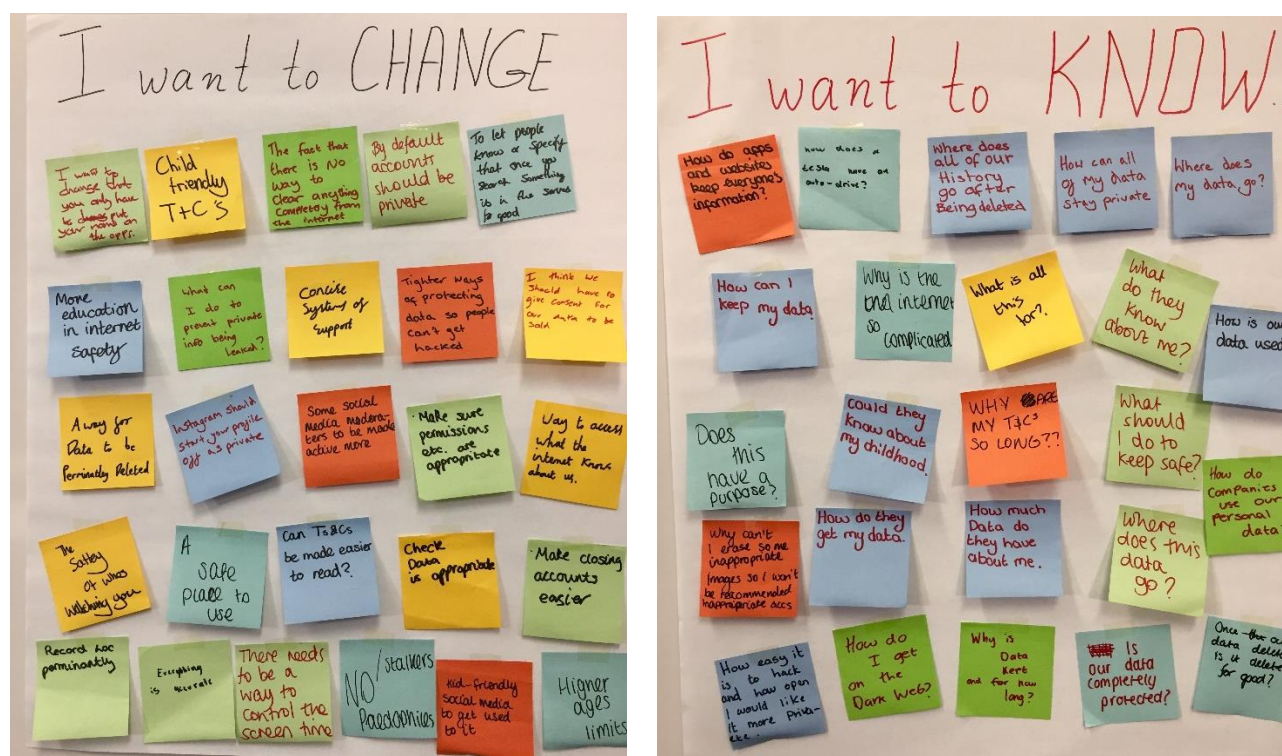
To facilitate the children's thinking about the future and about child development, we designed an activity, 'Advice to a younger sibling' (see Figure 5), where the children write a message to an imaginary younger sibling, telling them what they need to learn about privacy online. This exercise worked well, but the children still struggled to express what effective strategies might be.

Figure 5: Imagine that you have a younger sister or brother. What would you like them to know about privacy online by the time they are your age?



Finally, we felt that some questions remained unanswered and we gave children the opportunity to ask any questions they still might have and make suggestions for changes in the future (see Figure 6). This worked well, and we will be using this input in the design of the online toolkit.

Figure 6: What do you want to know? What do you want to change?



The focus groups for parents and teachers covered the same issues discussed with the children, but with greater emphasis on adults' privacy knowledge, professional/ parenting practices, the school's approach to privacy and perceived harm and responsibilities.

Child juries

One of the outputs from the project is an online toolkit to support and promote children's digital privacy skills and awareness. The toolkit is aimed at children of secondary school age, parents and educators, and was developed with the participation of a mix of children in Years 8 and 10. With the help of experts and practitioners, we collected the best resources on online privacy and organised three child juries in March 2019 with a total of 18 children. The children were given the opportunity to assess the resources and help design the online toolkit.

The juries started with gathering children's ideas on what the toolkit should look like and what it might include, also reviewing example models of toolkits (e.g., BBC Own It). Then the children were given the opportunity to engage with the individual resources and to rate them based on their suitability and age-appropriateness (see Figure 7). Finally, the juries discussed suggestions and recommendations for industry, policy-makers and educators. The children then voted for recommendations derived from the focus group findings.



Figure 7: Resource assessment form (child juries)

year 8

Work station 2 MY FEEDBACK

Age: *13* Year group: *year 8* Gender: *f*

| Resource | My overall rating How would you rate this resource? ☺ Like it very much ☹ It's OK ☹ Don't like it (circle one for each row) | Age group What age group is this suitable for? |
|--|--|--|
| 8. The spy in my pocket | ☹ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) <u>Older children</u> |
| 9. Terms & Conditions Quiz | ☺ ☹ ☹ | 1) Any age 2) <u>My age</u> 3) Younger children 4) Older children |
| 10. Trace my shadow | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 11. King GAFA | ☺ ☹ ☹ | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |
| 12. Top tips for minimising children's data footprints | ☺ ☹ ☹ | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |
| 13. Ethics and the Law: data protection | ☺ ☹ ☹ | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |
| 14. Simplified social media Terms and Conditions | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 15. Do you have a sharent in your life? | ☺ ☹ ☹ | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |
| 16. How well do you know your privacy rights? | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) <u>Older children</u> |
| 17. Teen Action Kit | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| Game 1: Band runner game | ☺ ☹ ☹ | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |

Fun but pointless

Work station 2 MY FEEDBACK

Age: *13* Year group: *year 8* Gender: *f*

| Resource | My overall rating How would you rate this resource? ☺ Like it very much ☹ It's OK ☹ Don't like it (circle one for each row) | Age group What age group is this suitable for? |
|--|--|--|
| 8. The spy in my pocket | ☺ ☹ ☹ <i>Boring</i> | 1) Any age 2) <u>My age</u> 3) Younger children 4) Older children |
| 9. Terms & Conditions Quiz | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 10. Trace my shadow | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 11. King GAFA | ☺ ☹ ☹ <i>children</i> | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |
| 12. Top tips for minimising children's data footprints | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 13. Ethics and the Law: data protection | ☺ ☹ ☹ <i>video</i> | 1) Any age 2) <u>My age</u> 3) Younger children 4) Older children |
| 14. Simplified social media Terms and Conditions | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 15. Do you have a sharent in your life? | ☺ ☹ ☹ | 1) Any age 2) My age 3) Younger children 4) Older children |
| 16. How well do you know your privacy rights? | ☺ ☹ ☹ <i>misleading</i> | 1) Any age 2) My age 3) Younger children 4) <u>Older children</u> |
| 17. Teen Action Kit | ☺ ☹ ☹ <i>thought it be hard info</i> | 1) Any age 2) My age 3) Younger children 4) Older children |
| Game 1: Band runner game | ☺ ☹ ☹ | 1) Any age 2) My age 3) <u>Younger children</u> 4) Older children |

Part II: The research process

Ethics approval

The project received ethics approval from the Research Ethics Committee at the London School of Economics and Political Science (LSE) following a thorough review of the research design and methodology, ethical issues and safeguards, participant consent, confidentiality and anonymity, sensitivity of data, assessment of risk to the participants and researchers, and data management plans.

The proposal also underwent a data security review involving approval of the process of data production and access, quality assurance, back-up and security procedures, data management and curation, data sharing, consent, anonymisation and strategies to enable further re-use of data, and copyright and intellectual property ownership. All project members were subject to enhanced Disclosure and Barring Service (DBS) checks, and the certificates were presented to the participating schools prior to gaining access to the research sites. In Scotland, additional approval from the local council was required and obtained.

Recruitment

We decided to include children aged 11 to 16 (Years 7, 9 and 11, or S1, S3 and S5 in Scotland), their parents and educators in several secondary schools across different parts of the UK. These ages were selected because Year 7 marks the sometimes-risky transition to secondary school; Year 9 marks the age at which currently information society services cease to require parental consent; and Year 11 marks the level of maturity proposed by the General Data Protection Regulation (GDPR) for child consent. While conducting the research, we were sensitive to variation and progression in maturity and understanding across the age groups, and were also concerned to identify variation in digital understanding within each age group.

The schools were recruited via snowballing from personal contacts (via local authority members, school governors or teachers) and selected avoiding high-performing schools. A school invitation letter was sent to each school, accompanied by full details about the project and the research staff. Information sheets and consent forms were sent to the pupils, parents and teachers via the school. The participants were put forward by the school from the children who volunteered.

Our requirement for the selection process was to allow for maximum diversity as much as possible, including school performance and digital skills, as well as socioeconomic and ethnic background. We aimed for an equal number of boys and girls. We also recruited parents from two of the fieldwork sites and teachers from three of the schools. We asked all schools to put us in touch with parents and teachers, but this was not always possible to organise due to the busy schedules of both the schools and the potential participants. In total, we spoke to 151 students, 20 parents and 16 teachers across the country. We also worked with 18 children to design the online toolkit.

Data collection

We held focus groups with pupils from six secondary schools in the UK (two in London and one each in Essex, the Midlands, Wales and Scotland). All sessions were held on the school premises in a quiet location, allowing for unobstructed and anonymous conversation. We carried out 28 mixed-gender focus groups with children aged 11–12 (Year 7), 13–14 (Year 9) and 15–16 (Year 11), 15 interviews with children (and parents), and 3 child juries, adding up to a total of 169 student participants across the country (85 girls, 84 boys). The focus groups with children lasted 73 minutes on average (anything between 40 minutes and 2 hours 20 minutes, with a total of 34 hours 16 minutes of focus group discussions with children). The juries with children lasted 2 hours.

We held focus groups with teachers in two schools (Essex and London), and interviews with teachers in two schools (the Midlands and Scotland), as well as a focus group with parents in one London school and interviews with parents and children in another. We spoke in total to 20 parents of children in secondary school and to 16 teachers. We originally envisioned only focus groups with the parents and teachers, but added interviews to allow for more flexibility around their busy schedules.

The focus groups with teachers were 56–57 minutes long, and the one with parents was 1 hour 27 minutes. The interviews with teachers were between 20 minutes and 1 hour 7 minutes (a total of 240 minutes). The interviews with parents and their child were between 14 minutes and 52 minutes (average of 32 minutes, 6 hours 48 minutes in total). The different duration was based on the availability of the participants.

All focus groups were audio recorded; some photographs were taken with the consent of the child participants and their parents. Once collected, the audio recordings were transferred to a secure computer server at LSE. After a successful transfer check, the data was erased from the recording devices. In keeping with minimum project auditing requirements, we are securely storing the documents with personal data (names and signatures on the consent forms) for the required period of 10 years, after which the forms will be securely destroyed.

The interviews and focus group discussions were transcribed by a vetted GDPR-compliant external transcriber (Way with Words), where only audio recordings were provided and securely transferred. The transcription agency ensured us that it was securely storing the data for the duration of the project, and then erased all project-related data promptly at the end of their service period.

The names and details of the schools and participants were anonymised immediately after receiving the transcripts, and the anonymised details were used on any notes taken. No data that has not been anonymised completely will be shared with third parties. We have taken measures to ensure the confidentiality and anonymity of the participants. Names of respondents and any possible identifying information have been changed, altered or redacted from the transcripts. Extracts of carefully anonymised data will be used in the future for the purposes of presentations, publications etc.

Participants

We aimed for diversity in relation to socioeconomic background, ethnicity and digital skills across the sample, and an approximately similar number of male and female participants across all categories (children, parents and teachers). For the child participants we also wanted equal number across the three age groups. This was not always possible. We managed to interview a similar number of boys and girls (85 girls, 84 boys) and the same number of children in Years 7 and 9 (49 in each year group), but a slightly smaller number of children in Year 11 (35). Two children at the end of their Year 10 took part during the pilot research as children in Year 11 were already on a summer break. We were also able to speak to more female parents (15 mothers, 5 fathers) but more male teachers (11 male and 5 female). While the sample included a mixture of socioeconomic backgrounds and digital skills amongst the children and parents, the majority of the participants were white.

Table 1: Participants

| Location | Research methods | | Number of participants | Duration of the sessions |
|----------|--------------------------------|----------------------|---|---|
| London | FGDs with children (n=6) | | 28 children (14 girls, 14 boys) | |
| | | <i>Year 7 (n=3)</i> | <i>16 children (10 girls, 6 boys)</i> | 1h30' 1h54' 2h20' |
| | | <i>Year 9 (n=2)</i> | <i>10 children (3 girls, 7 boys)</i> | 57' 1h31' |
| | | <i>Year 10 (n=1)</i> | <i>2 children (1 girl, 1 boy)</i> | Joint with one of the Year 9 groups |
| | FGD with parents (n=1) | | 3 parents (3 female) | 1h27' |
| | FGD with teachers (n=1) | | 6 teachers (5 male, 1 female) | 57' |
| | Parent–child interviews (n=15) | | 16 children (10 girls, 6 boys), 17 parents (5 male, 12 female) | Between 14' and 52'; total of 408' (6h48') |
| | Child juries (n=3) | | 18 children (5 girls, 13 boys) | 2h |
| Midlands | FGDs with children (n=6) | | 34 children (16 girls, 18 boys) | |
| | | <i>Year 7 (n=2)</i> | <i>9 children (4 girls, 5 boys)</i> | 45' 43' |
| | | <i>Year 9 (n=2)</i> | <i>11 children (4 girls, 7 boys)</i> | 51' 55' |
| | | <i>Year 11 (n=2)</i> | <i>14 children (8 girls, 6 boys)</i> | 52' 45' |
| | Interviews with teachers (n=3) | | 3 teachers (all female; two were interviewed together) | 20' 23' |
| Essex | FGDs with children (n=6) | | 27 children (13 girls, 14 boys) | |
| | | <i>Year 7 (n=2)</i> | <i>10 children (5 girls, 5 boys)</i> | 59' 40' |
| | | <i>Year 9 (n=2)</i> | <i>9 children (4 girls, 5 boys)</i> | 1h27' 1h23' |
| | | <i>Year 11 (n=2)</i> | <i>8 children (4 girls, 4 boys)</i> | 1h12' 1h13' |
| | 1 FGD with teachers (n=1) | | 3 teachers (male) | 56' |
| Wales | FGDs with children (n=4) | | 21 children (11 girls, 10 boys) | |
| | | <i>Year 7 (n=1)</i> | <i>6 children (4 girls, 2 boys)</i> | 56' |
| | | <i>Year 9 (n=2)</i> | <i>9 children (5 girls, 4 boys)</i> | 1h56' |

| | | | |
|----------|--------------------------------|---|------------------------------|
| | | | 1h58' |
| | | Year 11 (n=1) | 6 children (2 girls, 4 boys) |
| Scotland | FGDs with children (n=6) | 25 children (16 girls, 9 boys) | 1h51' |
| | Year 7 (S1) (n=2) | 8 children (7 girls, 1 boy) | 1h12' |
| | | | 1h13' |
| | Year 9 (S3) (n=2) | 10 children (5 girls, 5 boys) | 1h26' |
| | | | 1h21' |
| | Year 11 (S5) (n=2) | 7 children (4 girls, 3 boys) | 1h20' |
| | | | 1h19' |
| | Interviews with teachers (n=4) | 3 male, 1 female | 1h7' |
| | | | 1h4' |
| | | | 23' |
| | | | 43' |
| | | | |
| All | FGDs with children (n=28) | 135 children (70 girls, 65 boys) | 34h16' |
| | FGDs with teachers (n=2) | 9 teachers (1 female, 8 male) | 1h53' |
| | FGDs with parents (n=1) | 3 parents (female) | 1h27' |
| | Parent-child interviews (n=15) | 16 children (10 girls, 6 boys), 17 parents (12 female, 5 male) | 6h48' |
| | Interviews with teachers (n=7) | 16 teachers (5 female, 11 male) | 4h |
| | Child juries (n=3) | 18 children (5 girls, 13 boys) | 2h |

Note: FGD = focus group discussion.

Data analysis

A coding frame for the data analysis was developed based on the conceptual framework. It was tested by three researchers and revised. Additional codes emerging from the data analysis were added where necessary. The consistency of the coding procedure was ensured by separate coding (of two transcripts) carried out by three researchers and comparisons of the coding practice, discussing any differences and refining the coding approach. The remaining transcripts were coded by two of the researchers, and a sample was checked by the third researcher. Any issues emerging during the coding process were discussed by the team and addressed accordingly.

Coding framework

Thematic codes

01. Interpersonal privacy (data given, data given by others)
02. Institutional privacy (data given, traces, profiling)
03. Commercial privacy (data given. traces, profiling)
04. Keep to myself
05. Other privacy definition, value, importance
06. Privacy actions, tactics

07. Privacy literacy and skills
08. Child development
09. Gender
10. Regulation and rights
11. Technological innovation
12. Parental mediation
13. Risk and harm
14. Support and guidance
15. Golden quote

Activity codes

Activity 1 (introduction)

Activity 2 (my apps, sites, and privacy)

Activity 3 (privacy terms)

Activity 4 (my data)

Activity 5 (my data shadow)

Activity 6 (privacy strategies and support)

Activity 7 (letter to sibling)

Activity 8 (ask or recommend)

Activity 9 (anything else)

Administrative codes

Coding by demographic

Part of the country

Year group

Type of participant (child, teacher, parent)

Appendix

| | | |
|--|---|---|
| <p>Activity 1: Introduction</p> <p>10 minutes</p> <p>All together</p> <p>Need:</p> <ul style="list-style-type: none"> - name stickers - coloured pens - audio recorder | <p>Hi, thanks for coming – we’re excited to speak with you! Does everyone have their consent form signed by you and your parent? [Check for and collect consent forms]</p> <p>I’ll give you a name sticker – please write your FIRST name on it in BIG writing and stick it on you. [Hand out stickers and pens in 2 or 3 colours, put on own stickers and introduce ourselves]</p> <p>We’re from the London School of Economics, a university in the middle of London. We’re audio-recording today’s discussion, as you can see. We’re interested to learn which apps and devices you use for the internet, and what you share about yourself online. What you say, together with other students around the country, will help us write a report for the government, and create an online toolkit for children and young people to learn about internet privacy. The aim is to make the internet a safer and better place. Today’s discussion will take about 1.5 hours. [Adjust as appropriate, depending on activities selected]</p> <p>Everything we discuss today will stay completely confidential. Nothing will get back to your teachers or your parents. We’ll anonymise what you say when we write up our report. If there’s anything you don’t want to answer, that’s fine. Please keep what other people have said here confidential too. [Turn on audio-recorder]</p> <p>So, what do you think this is going to be about? What comes to your mind when we say privacy and the internet? [Get them talking]</p> <ul style="list-style-type: none"> - What does it mean to be ‘private’ online? - Some people talk about ‘personal data’. Do you have ‘personal data’? What might that be? - Do you do anything to keep your privacy online? From whom? - Is privacy online important to you? What about offline? | <p>Probes:</p> <p>What did your teacher tell you about what would happen today?</p> <p>Have you seen anything on the news recently about ‘privacy online’?</p> |
| <p>Activity 2: My apps, sites and privacy</p> <p>15 minutes</p> <p>All together</p> | <p>First, we’d like you to list all the apps and websites you used over the last week. Use one post-it for each item. [Hand out packs of post-its, give them 5 minutes to work individually. Put A1 posters in the middle]</p> <p>Please stick your post-its on the A1 posters in the middle – put them anywhere. [Invite explanations... what’s that for? ... as they are sticking on their post-its]</p> | <p>Apps:</p> <p>Gaming (Minecraft, Clash of Clans, Clash Royale, CRS racing, Fifa, Grand Theft Auto, Pokémon Go, Friv, Club Penguin, Roblox)</p> <p>Social media (Instagram, Snapchat, Twitter, Reddit, Pinterest, Facebook)</p> |

| | | |
|--|---|---|
| <p>Need:</p> <ul style="list-style-type: none"> - post-its - pens - A1 posters | <ul style="list-style-type: none"> - Have we missed any apps or websites? What about at school or other places you go? - How do you choose which apps to use? - Anything here you've just started using? - Anything that you were using before but not anymore? Why not? - When using an app/website for the first time, what are the things you want to know about it? - How do you decide which to trust? - Have you changed the default settings? Why? - Do you read their terms and conditions? Why? What are you looking for? - [Pick a popular app] What do you think should be the age to use this app? Why? - What is the right age to decide independently? - Among all these apps, do any have privacy settings that are easy to use? Any settings a problem? | <p>Chat (Discord, Kik, Hangouts, WhatsApp, Viber, Skype)</p> <p>Live/web streaming (Musical.ly, Omegle, Tumblr, Steam, Twitch, Spotify, YouTube, Netflix)</p> <p>Selling/buying apps (Amazon, eBay, ASOS)</p> <p>Websites (Google, BBC Bitesize, for home, for school, school intranet, school homework site for fun, to register for something, for info...)</p> |
| <p>Activity 3: Privacy terms (optional) 15 minutes</p> <p>All together</p> <p>Need: - cards</p> | <p>Now let's play a card game. I have a deck of cards – each has a word written on it. I will put them on the table one at a time. Please tell me if you have heard of the word and what it might mean. Most of the words are quite difficult, so it's absolutely fine to say you haven't heard of it or are unsure what it means.</p> <p>[Place the cards on the table one by one, prompt for explanations of each, encourage the children who do not know it to say so]</p> <ul style="list-style-type: none"> - First time hearing this word? Unsure what it means? - Where have you heard/seen this word? - When did you first hear this word (how old were you then)? - What does it mean? What else do you know about it? | <p>Cards: cookies, privacy settings, facial recognition, geo-location, digital footprint, dark web, algorithms, artificial intelligence, encryption</p> |
| <p>Activity 4: Data cards 20 minutes</p> <p>Small groups (divide by pen colours into two groups)</p> | <p>Now let's think about the data we share online and who it is shared it with. I have 13 cards with different types of data. I will give them to you one at a time, and you need to decide if you are happy to share this data with: 1) Your online contacts; 2) Your school, GP, future employer; 3) Companies (for advertising or profiling); or 4) You want to keep to yourself. You can put the same card in more than one place.</p> <p>[Check they understand; give one data type (four identical cards) at a time; probe for explanations, disagreements, variation within one card] [Put an A1 poster page in the middle to write additional notes]</p> <ol style="list-style-type: none"> 1. Who would you share this with and why? | <p>Probes: discuss these activities as they are done (purpose of this exercise is talk, not writing)</p> <p>1. Your name? Age? Fake age? Photographs [showing what?], snaps, locations, status updates, date of birth; check-in to places, on different sites. What if you do a quiz?</p> <p>2. As above. Also sharenting, tagging.</p> |

| | | |
|---|--|---|
| <p>1. Data given</p> <p>2. Data given by others</p> <p>3. Data traces</p> <p>Need:</p> <ul style="list-style-type: none"> - data cards - A1 posters | <ul style="list-style-type: none"> - How do you decide what to post (and where)? Why? What don't you post or share? - Looking at all the data on the table, does that seem a lot about you, or not too much? - What else might you put in the 'keep to myself' pile? <p>2. Now, let's think if we need to move some of the cards on the table. Think about all the information that others share or post online about you. Let's start with friends, other people at school. Who else? Parents? Teachers/the school? Doctor? [Check if cards need to be moved from 'Keep to myself']</p> <ul style="list-style-type: none"> - How different is this to what you share? - Could anyone get information about you from what your friends share, even if they do not mention you? - How do you feel about this? - Can you think of a situation where something was shared that you didn't want shared? - Having to share a device? <p>3. Now, let's think again if more cards need to be moved. Do your apps collect other information about you, in addition to the things that you or others post on them? Maybe information that the apps and devices collect without you realising? [More prompting may be needed; check again about moving cards]</p> <ul style="list-style-type: none"> - Do they track how long you use an app for? Do they know where you are? - What if you log into an app or website using a Facebook or Google login? - What if you use devices like internet-connected toys (e.g., drone), games console (Xbox), Smart home devices (Alexa, Google Home), fitness tracker (Fitbit), VR headset? - What do they use this information they collect for? - Can it be used to target advertising to you? How? | <p>SIMS (computer where teachers record and track your attendance and performance)</p> <p>3. Data collected via your library card or school ID? Bus pass or Oyster card. CCTV around the school</p> <p>Cookies and trackers. Geo-location, time zone, language, IP address, shop loyalty cards; being tracked via Google Maps?</p> <p>Facial recognition? Thumbprint to pay for dinner or unlock phone? Biometric? Biased algorithms?</p> <p>Personalise ads, offer games or promotions</p> <p>Analyse trends (data profiling, social credit score)</p> <p>Sell access to your data (data brokers)</p> <p>Prompt for understandings of the internet – who is they, how does it work, where's the power?</p> |
| <p>Activity 5:</p> <p>Data profiling</p> <p>10 minutes</p> <p>Still in groups but working individually</p> | <p>Spontaneous reflections on data profiling:</p> <p>Do you think the internet can work out things that you may not have said directly?</p> <ul style="list-style-type: none"> - If we Googled your name, what could we find? - What can apps work out about you that you didn't mean to tell them? - Can these apps 'guess' things about you like your favourite TV show or game? [How?] - How do you think they do that? Why? How long do they keep this info for? - Why is this information valuable to them? Why valuable to you? <p>So maybe the internet knows quite a lot about you! [Mix all data cards in one pile to show flow of info]</p> | <p>Age, gender, education</p> <p>Who your friends are? What you like?</p> <p>Where you go, what you spend time on?</p> <p>Spending</p> <p>Health, ill health (e.g., asthma), learning difficulties</p> <p>Religion, ethnicity, sexuality, politics</p> <p>Your parents' politics? Or income?</p> <p>How you're doing at school?</p> <p>What you search for? Browsing history...</p> |

| | | |
|--------------------------------------|--|---|
| <p>Need: - worksheets</p> | <p>It seems that the internet can work out things that you may not have said directly by using different types of data, including from other people like you. This is called data profiling. Companies and sometimes governments gather data from many people and match who you are like and then they can make predictions about you. [Explain and seek reaction]</p> <p>Further reflections on data profiling:</p> <ul style="list-style-type: none"> - Did you know this was possible? How do you think it works? - Who might do this profiling and why (what might they use it for)? - How do you feel about what the internet knows about you? - Anything you might be worried about (now/ future)? - Anything embarrassing? - It's sometimes said that young people don't care much about their privacy – do you agree? - Or that you'll give away personal information to be able to use a site or app for free...? If an app offers you money to track everything you do online, would you sign up? <p>Harms:</p> <ul style="list-style-type: none"> - Does anything worry you about your online privacy? What? Why? What could go wrong? - Have you been upset by something that someone else posted or shared about you? - Have you ever changed your mind about what you've posted? Or regretted it? - Can you think of an example where something has gone wrong? - Is there anything you can do to put things right when there's a problem? - How might this affect you if trying to get a job in the future or a university place? - Data being hacked and shared for fraud? - Database mistakes and errors hard to put right <p>But maybe the internet doesn't know everything, or gets some things wrong. Please write down: [Hand out worksheets]</p> <ol style="list-style-type: none"> 1) Who the internet thinks you are 2) What it gets wrong about you 3) Things it doesn't know about you | <p>Focus: knowledge of data processing, flow, monetisation, profiling, data brokers, data intermediaries</p> |
|--------------------------------------|--|---|

| | | |
|--|--|---|
| <p>Activity 6: Privacy strategies and support</p> <p>15 minutes</p> <p>All together if group is small but stay in groups if large</p> | <p>Let's think about some of things you do online to protect or control your personal information: [Prompt for lots of ideas]</p> <ul style="list-style-type: none"> - Maybe you've recently updated your privacy settings on your favourite apps? Discuss how/why. - Are there things you do to control your information online? - Any clever tips? Do they work? How do you know? - Things your parents do to protect your privacy online? How do you feel about it? When should you become independent? - Are there things you feel you can't control or manage? (e.g., account with forgotten password) <p>Learning and help:</p> <ul style="list-style-type: none"> - Have you ever asked someone to help you with a problem (remove a photo, block someone, stop something being shared)? - Who do you ask...? - Formal learning: any formal teaching (citizenship or computing class, PSHE)? - Informal learning: friends or family, online, just pick it up or work it out yourself? | <p>Privacy tactics:</p> <p>Share passwords?</p> <p>Read privacy/cookie policy? Adjust privacy settings?</p> <p>Delete cookies? Use ad-blocker? Do not track?</p> <p>Use privacy-protecting browser?</p> <p>Unsubscribe, delete account?</p> <p>Stop using apps/sites/internet?</p> <p>Delete info/post less?</p> <p>Refuse/post inaccurate personal info?</p> <p>Limit who can see your data?</p> <p>Use incognito windows</p> <p>The dark web (what's that? How does it work?)</p> <p>Encrypted sites e.g., WhatsApp</p> |
| <p>Activity 7: Advise others OPTIONAL 5 minutes Need: - worksheets</p> | <p>Imagine that you have a sister or brother who is five years younger than you are. Think about all the things you would like them to know in the next five years, by the time they are your age. Write them a message, telling them all the things they should know about privacy and the Internet.</p> <p>[Hand out worksheets]</p> <p>[Summarise what they have said before moving to the next activity]</p> | |
| <p>Activity 8: Questions?</p> <p>10 minutes</p> <p>All together</p> | <p>With everything you've shared with us today, you must have lots of thoughts and questions about how you use the internet!</p> <p>1. What would you like to know about your online information and privacy? Can you write down your questions? We'll try to find the answers and create a resource for young people (and schools).</p> | <p>Do you feel like you have enough information to help protect your personal privacy?</p> <p>Should companies be able to collect your data?</p> |

| | | |
|--|--|--|
| <p>Need:</p> <ul style="list-style-type: none"> - post-its - A1 posters | <p>[Hand out post-its. Stick up A1 poster (heading: 'What I want to know'). Get them to put their post-its on the wall. Try to answer some of their questions as part of the conversation]</p> <p>OPTIONAL</p> <p>2. Are there things that the people/companies who designed the apps and devices should do differently to make privacy better? [Hand out post-its. Stick up A1 posters (heading: 'What industry should do'). Put post-its on wall]</p> <ul style="list-style-type: none"> - Should the industry (e.g., Instagram, Apple, Google) consult children when designing sites and apps and devices? - What would you tell them? | <p>Any kinds of data they shouldn't be allowed to collect or keep? (sensitive? Facial recognition?)</p> <p>Should they change how people can tag you? Or how parents can monitor what you do online?</p> <p>Should they make it so parents have to give consent to what you do online?</p> <p>Should there be a minimum age for some sites/apps? Which/what?</p> |
| <p>Activity 9:</p> <p>Thanks</p> <p>10 minutes</p> <p>All together</p> | <p>Thank you! This was really interesting and helpful for us. We don't know all the answers either, but we'll find out what we can and we'll send what we learn to your school.</p> <ul style="list-style-type: none"> - How did you find the discussion? Anything you enjoyed? - Anything we should change when we visit the next school – anything boring or unclear? - Anything that would be more interesting or fun? <p>Thanks for that! We'll keep this in mind for the next time.</p> <p>If students and their parents have agreed to photographs, please stay for five more minutes before you leave. [Everyone take off their name stickers first]</p> | |

References

- Coleman, S., Pothong, K., Perez Vallejos, E. and Koene, A. (2017) *The internet on our own terms: How children and young people deliberated about their digital rights*. 5Rights. Available at <https://casma.wp.horizon.ac.uk/wp-content/uploads/2016/08/Internet-On-Our-Own-Terms.pdf>
- Family, Kids, and Youth (2017) *Cyberbullying: Research into the industry guidelines and attitudes of 12-15 year olds*. Available at www.kidsandyouth.com/wp-content/uploads/2017/04/FKY-21.4.17Cyberbullying-Qualitative-Workshops-.pdf
- Kleine, D., Pearson, G. and Poveda, S. (2016) *Participatory methods: Engaging children's voices and experiences in research*. London: Global Kids Online. Available at www.globalkidsonline.net/participatory-research
- Greene, S. and Hogan, D. (2005) *Researching children's experiences: Methods and approaches*. London: Sage Publications.
- Nissenbaum, H. (2004) 'Privacy as contextual integrity.' *Washington Law Review* 79, 1119–58.
- Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) *Children's data and privacy online: Growing up in a digital age. An evidence review*. London: London School of Economics and Political Science. Available at www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf
- van der Hof, S. (2016) 'I agree, or do I? A rights-based analysis of the law on children's consent in the digital world.' *Wisconsin International Law Journal* 34(2), 409–45.